Dell EMC Integrated Data Protection Appliance

Version 2.2

Product Guide

302-004-956

REV. 01

DELL EMC

Published June 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Revision history

Table 1 IDPA 2.2 Product Guide revision history

Revision	Date	Description
01	June 2018	Version 2.2

CHAPTER 1

Introduction

This chapter provides a general overview of the Integrated Data Protection Appliance 2.2 features and hardware configurations.

Topics include:

Document scope and audience

The scope of this document is to describe the administrative details of the Integrated Data Protection Appliance (IDPA).

The target audience for this document includes field personnel, partners, and customers responsible for managing and operating the IDPA. This document is designed for people familiar with Dell EMC Data Protection solutions.

Product features

The IDPA provides a simplified configuration and the integration of data protection components in a consolidated solution.

Simplified deployment and configuration
The IDPA model DP4400 is a hyperconverged, 2U system that a user can install and configure onsite.

The system software for each component is installed and configured to the greatest extent possible before the appliance is shipped. A backup application, target storage, reporting and analytics, search, appliance configuration manager (ACM) come embedded on the appliance.

This release includes the IDPA System Manager and adds the optional Cloud Disaster Recovery (CDRA) to the software stack.

Centralized management
The ACM provides a graphical, web-based interface for configuring, monitoring, and upgrading the appliance. IDPA System Manager provides advanced monitoring and management capabilities of the IDPA from a single pane of glass and includes the following features:

- Comprehensive dashboards that include the following Avamar and IDPA system information:
  - Backup activities
  - Replication activities
  - Capacity
  - Health
  - Alerts
- Monitoring multiple systems capabilities including system health and activities.
- Management capabilities for the backup application.
- Advanced search and recover operations through integration with Search.
- Reporting capabilities.

Backup administration
The IDPA protects virtual and physical clients, different types of file systems, applications, and databases.

Monitoring and analytics
The reporting and analytics feature offers robust reporting functionality with dedicated sections for various features. The reports help you retrieve information about the environment so that you can review and analyze the activities in the environment. Using these reports, you can identify outages in the environment, diagnose problems, plan to mitigate risks, and forecast future trends. You can run

custom and system report and dashboard templates on demand or on a schedule at defined time intervals, per the enterprise requirements.

The ACM dashboard displays a summary of the configuration of the individual components and allows the administrator to monitor the appliance, change configuration details, or upgrade the system and its components. The dashboard also displays appliance health alert information for the server and VMware components.

Search
The Search feature provides a powerful way to search backup data within the IDPA and then restore the backup or download the search results. Scheduled collection activities are used to gather and index the metadata, which is then stored within the IDPA.

Disaster recovery
DD Cloud DR is an optional solution that facilitates the recovery of on-premises virtual machines by providing the capability to recover those VMs in the cloud. DD Cloud DR integrates with the backup application inside the IDPA to copy backups of virtual machine data to the public cloud. It can then perform DR tests or failover of production environments by orchestrating a complete conversion of the VM to an Amazon Web Services Elastic Compute Cloud (EC2) instance, and by running this instance in the cloud.

The CDRA is a built-in application that manages deployment of the necessary infrastructure to the cloud, copying of virtual machine backups to the cloud, and orchestrates the compression, encryption and copying of the backed-up VM data to the cloud.

Note

CDRA is optional.

Scalability
The IDPA is designed to be scalable so it can grow with changing needs. The base DP4400 configuration includes 24TB of storage space, which can be expanded by licencing additional capacity in increments of 12TB up to a maximum of 96TB.

Unified support
The same Customer Support team supports both the hardware and the software used in the appliance.

Note

The IDPA is compatible with IPv4 enabled networks and does not support pure IPv6 or dual stack networks.

System architecture and components

The IDPA combines multiple data protection solutions into a single product.

Detailed configuration

The IDPA is available in the following models:

Table 2 Configuration options for each model

Model	Protection Storage model	Protection Storage configuration options (usable TB)	Backup Server	Avamar Accelerator Node for NDMP/NAS Backup (optional)
DP4400	Data Domain Virtual Edition	24, 36, 48, 60, 72, 84, or 96 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1)
DP5300	Data Domain 6300	34, 82, or 130 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1)
DP5800	Data Domain 6800	96, 144, 192, 240, or 288 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1–3)
DP8300	Data Domain 9300	192, 240, 288, 336, 384, 432, 480, 528, 576, 624, 672, or 720 TB	Avamar Grid: • One utility node • Three M1200 storage nodes (12 TB) • Two switches	NDMP Accelerator (1–4)
DP8800	Data Domain 9800	624, 672, 720 768, 816, 864, 912, 960, or 1008 TB	Avamar Grid: • One utility node • Four M1200 storage nodes (16 TB) • Two switches	NDMP Accelerator (1–4)

Embedded software

After initial configuration, the following software is deployed and configured:

- Data Domain Virtual Edition (DDVE)
- VMware vCenter Server VM (internal architecture platform on which the appliance runs)
- VMware ESXi
- Avamar Virtual Edition (AVE)
- Avamar Proxy VM
- Integrated Data Protection Appliance System Manager VM
- Data Protection Advisor
  - Application Server Host VM

    - Datastore Server Host VM
- Data Protection Search
    - Index Master Node Host VM
- DD Cloud DR CDRA virtual appliance (optional)
- Appliance Configuration Manager

System self-protection

The IDPA is configured to protect itself from data loss with the backup and storage applications included in the system. The system is are protected with self-defined and self-initiated backup jobs that are scheduled daily and have a 30-day retention period. The system metadata is protected using checkpoint backup to the internal target storage.

Network connectivity overview

When a range of IP addresses is used during the IDPA configuration, the IP addresses are assigned in a standard order. Use the table below to determine which IP address is allocated to a component.

The first column in each table, IP Range Allocation, is the value to add to the first IP address in the range.

Table 3 IP address range assignments for the DP4400

IP Range Allocation	Example	Component	Assigned Field
+0	`192.0.2.1`	vCenter	VMware vCenter Server VM
+1	`192.0.2.2`	Target storage	Data IP 1
+2	`192.0.2.3`	Target storage	Data IP 2
+3	`192.0.2.4`	Target storage	Data IP 3
+4	`192.0.2.5`	Backup application	Server IP
+5	`192.0.2.6`	Backup application	Avamar Proxy VM
+6	`192.0.2.7`	IDPA System Manager	IDPA System Manager VM
+7	`192.0.2.8`	Analytics and reporting	Application Server Host VM
+8	`192.0.2.9`	Analytics and reporting	Datastore Server Host VM
+9	`192.0.2.10`	Search	Index Master Node Host VM
+10	`192.0.2.11`	DD Cloud DR CDRA (optional)	Data Domain Cloud Disaster Recovery (DD Cloud DR) Cloud DR Add-on (CDRA) virtual appliance

CHAPTER 2

Monitor and manage the appliance

This chapter introduces the features and functionality of the ACM dashboard.

Topics include:

About the dashboard

The ACM dashboard allows you to manage settings for the appliance and individual components, update customer support information, and upgrade software for the appliance and its components.

To access the dashboard, type `https://<ACM IP address>:8543/` in a web browser and log in. The dashboard requires Google Chrome 64.0.3282.140 and later or Mozilla Firefox 47.2 and later.

Note

The dashboard is enabled only after configuration of IDPA.

The initial view displays the **Home** page and tabs for **Health** and **Upgrade**.

Basic management tasks

View system details, change the password of appliance components, and log out from the dashboard.

Changing the ACM password

1. Click the **Change Password** icon.
2. Type the **Current Password**.
3. Type and confirm the **New Password**.
4. Click **Change Password**.

Note

The password must contain 9–20 characters and include at least one of each type of supported character. The following types of characters are supported:

- Uppercase letters (`A–Z`)
- Lowercase letters (`a–z`)
- Numbers (`0–9`)
- Special characters: period (`.`), hyphen (`-`), and underscore (`_`)

The password must not include common names or usernames such as `root` or `admin`.

The password gets changed for the users in the following sequence:

1. ACM internal LDAP user `idpauser`.
2. Storage (DDVE) `sysadmin` user.
3. Backup Server (Avamar) users:
   a. OS `admin` and OS `root`.
   b. Avamar server users – `root`, `mcuser`, `repulser`, and `viewuser`.
4. Backup server proxy OS `root` user.
5. IDPA System Manager(DPC) users: OS `admin` and OS `root`.
6. Reporting and analytics (DPA) users: Application Server OS `root`, Datastore OS `root`, Application server `administrator`.

7. Search(DPS) OS `root` and search default LDAP `root` and `admin`.
8. Cloud disaster recovery(CDRA) `admin`password.
9. VCenter and ESXi `idpauser` password.
10. ACM root password.

Note

After changing the password, ACM users will be logged out and they need to login again using the updated password.

Viewing version and build details
Click the **Information** (**i**) icon. The **About** page displays details about the IDPA version and build number.

Logging out
Click the **Log Out** button.

ACM dashboard Home

The **Home** tab provides an overview of the status and settings for the IDPA and each component.

On the dashboard **Home** tab, you can view the network configuration and product details, manage the password, time zone, SMTP, SNMP, and NTP settings, and modify customer support information.

You can also configure LDAP, create and download log bundles, update the common password across all components, register components with Secure Remote Services (formerly ESRS), and install optional components (CDRA).

Note

Secure Remote Services configuration link is present under gear icon menu. Do mouse hover on the gear icon to list all the menu options.

If DPS or DPA failed during configuration, ACM does not stop whole configuration. The configuration process still continues until it finishes. After the configuration process is finished, ACM dashboard provides an option to configure the failed component (DPS or DPA).

Downloading the configuration details
To download a PDF containing the current details of the IDPA configuration, click the Adobe PDF icon.

Managing system components
The **Home** tab contains panels for each of the following:

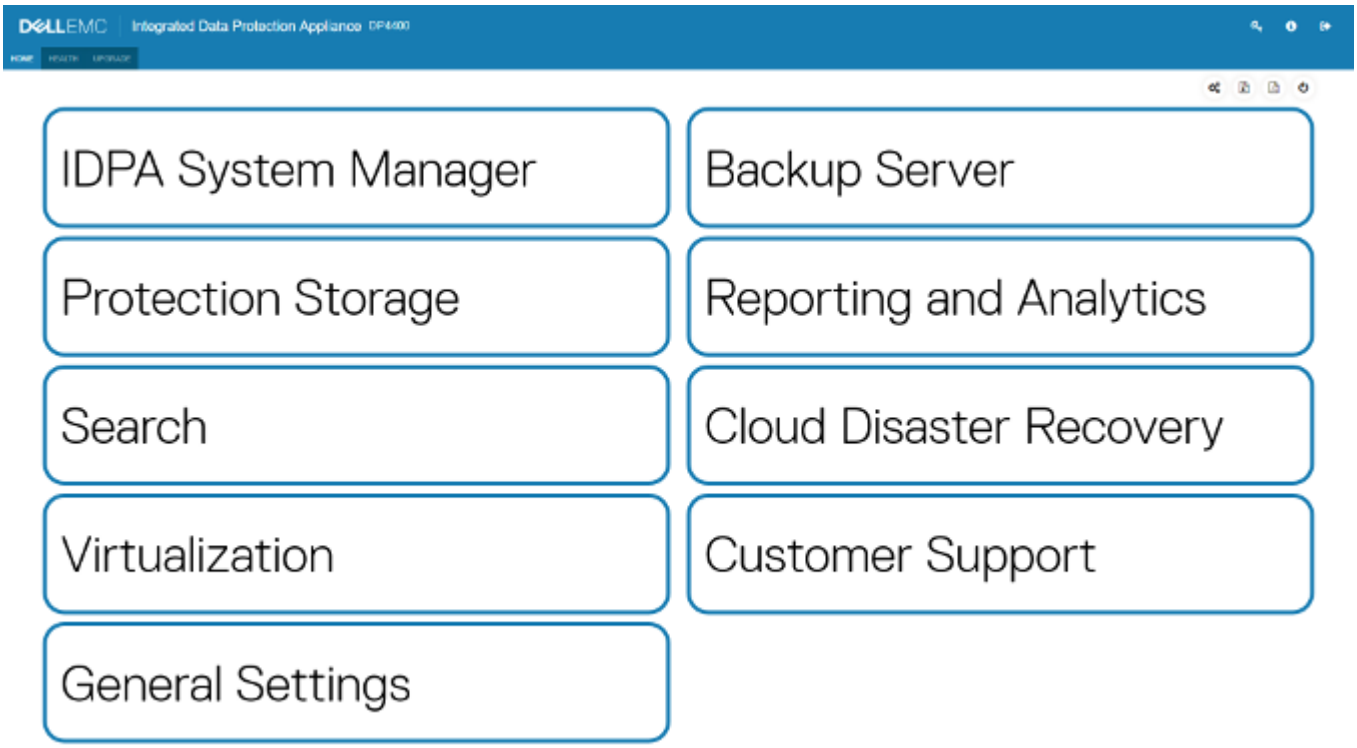
- **IDPA System Manager**
- **Backup Server**
- **Protection Storage**
- **Reporting and Analytics**
- **Search**
- **Cloud Disaster Recovery**
- **Virtualization**
- **Customer Support**

- **General Settings**

Note

If a component cannot be reached on the network or has an incorrect stored credential, the corresponding panel prompts the user to resolve the issue.

Figure 1 ACM dashboard home layout without individual panel details



Note

When ACM restarts, it tries to start each component. This may impact the speed with which the ACM UI is up and running.

IDPA System Manager panel

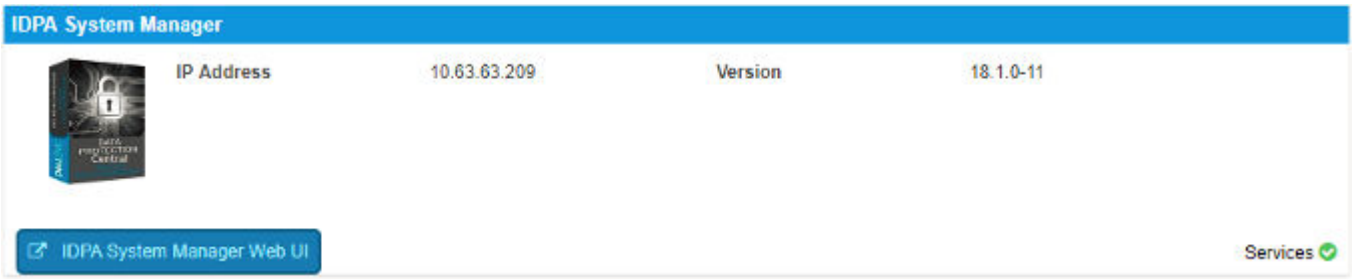
The **IDPA System Manager** panel displays the IDPA System Manager version and component IP address. To launch the **IDPA System Manager Web UI**, click the button and log in.

Note

If external LDAP has not been configured then use `idpauser` as username. If external LDAP has been configured then use LDAP username of the user.

Move the cursor to **Services** to view status information for IDPA System Manager services.

Figure 2 The **IDPA System Manager** panel on the ACM **Home** page



For more information about IDPA System Manager workflows and capabilities, refer to the *IDPA System Manager Administration Guide*.

Backup Server panel

The **Backup Server** panel displays the component IP address, Avamar version, total and available backup metadata storage, license status of the Backup Server node, and whether the installation of agents is in progress. Click the **Download Agents** link that appears after the agent installation finishes to load the Avamar Web Restore GUI, from which the Avamar agents can be downloaded.

Figure 3 The **Backup Server** panel on the ACM **Home** page

For more information about the role of backup agents and how to install them, refer to the *Avamar Administration Guide*. Move the cursor to **Services** to view status information for Avamar services.

Enabling certificate verification

By default, vCenter certificate checking is disabled on the IDPA.

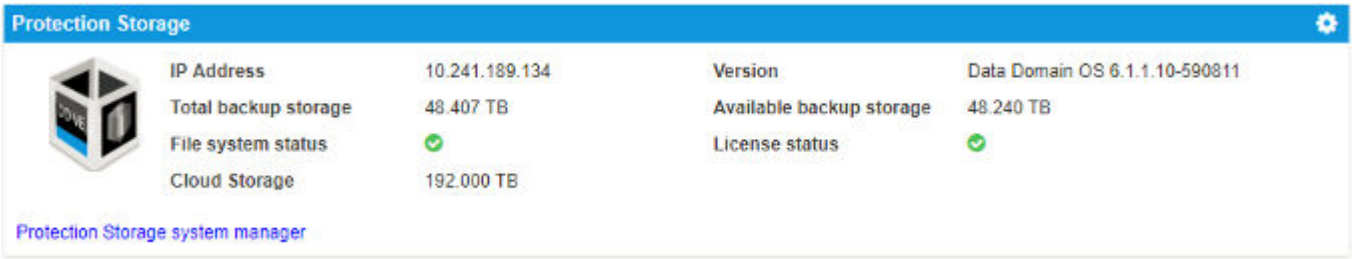
The IDPA uses a modified version of the Avamar `MCServer.xml` file. During configuration, this modification causes vCenter certificates to be ignored when adding vCenter servers. To enable certificate checking:

1. change the `ignore_vc_cert` value in the file to `false`,
2. restart the MC service using `dpnctl`,
3. stop `mcs` and `dpctl`, and
4. start `mcs` commands on Avamar server.

Protection Storage panel

The **Protection Storage** panel displays the DD OS version, component IP address, total and available backup storage, the file system and license status of the Protection Storage node, and any alerts requiring user action. To access additional functionality of the component, click the **Protection Storage System Manager** link.

Figure 4 The **Protection Storage** panel on the ACM **Home** page



Expanding storage capacity

You can add storage for Data Domain to expand the capacity of the Protection Storage node. Increasing the attached storage requires additional licensing.

Before you begin

- Obtain licensing for the increased storage capacity.

Once the system detects the hardware, the **Expand storage** option is available in the gear icon menu.

Procedure

1. In the **Protection Storage** panel, mouse over the gear icon on the top right and click the **Expand storage**.

   The **Storage expansion and license upgrade** wizard appears.
2. Click **Browse** and select the required license files for the additional storage.
3. Click **Expand**.

Results

After several minutes, the dashboard reflects the increased storage capacity.

Configuring cloud long-term retention feature on IDPA.

DD Cloud Tier is configured through ACM configuration. Follow the below procedures to create DD cloud units and configure Avamar back policies for cloud LTR.

Before you begin

Note

For detailed information on creating DD cloud units, refer *Data Domain Operating System Administration Guide*.

This process refers to the procedures in the following documents:

- *Data Domain Operating System Administration Guide* for DD OS 6.0 or higher
- *Avamar and Data Domain System Integration Guide* for Avamar 7.4 or higher

Procedure

1. On the **ACM** home tab, click the **Protection Storage System Manager** link.

   The **Data Domain System Manager** GUI is displayed.
2. Follow the "Importing CA certificates" procedure in the *Data Domain Operating System Administration Guide*.

   After importing the certificate, close the **Data Domain System Manager**.

3. Connect to the Avamar user interface through IDPA System Manager.

   The **Avamar Administrator** GUI is displayed.

4. Follow the "Adding or editing a Data Domain system with cloud tier support" procedure in the *Avamar and Data Domain System Integration Guide*.

   Note

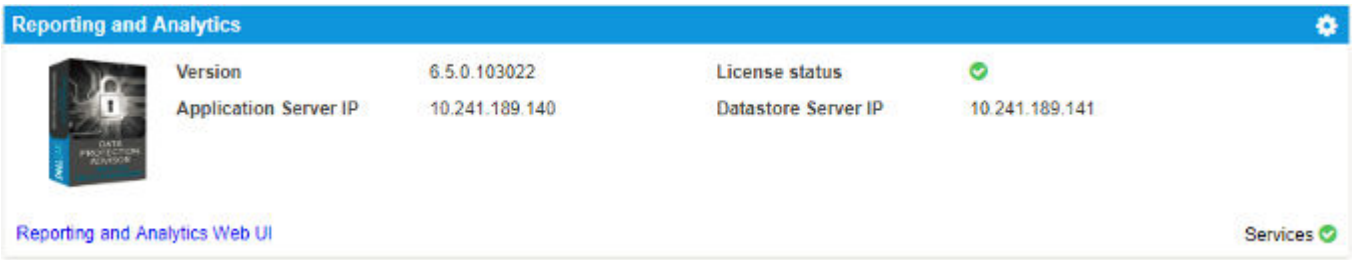
   The ACM makes the step that refers to "Adding a Data Domain system" unnecessary. To learn how to access the **Edit Data Domain System** dialog box, refer to "Editing a Data Domain system."

5. Follow the "Creating a new tier group" procedure in the *Avamar and Data Domain System Integration Guide*.
6. To verify your configuration, click the **Activity** launcher button in **Avamar Administrator** and review the list of session on the **Activity Monitor** tab.

Reporting and Analytics panel

The **Reporting and Analytics** panel displays the DP Advisor version, IP addresses for the Application Server and Datastore Server, the license status of the Reporting and Analytics node, and any alerts requiring user action. To load the Reporting and Analytics console, click the **Reporting and Analytics Web UI** link. Move the cursor to **Services** to view status information for DP Advisor services.

Figure 5 The **Reporting and Analytics** panel on the ACM **Home** page



If DP Advisor was not configured during the initial configuration process, the panel displays a message indicating Reporting and Analytics is not configured. To configure the Reporting and Analytics node, click the message. The Reporting and Analytics Configuration screen appears. On the **Reporting and Analytics Configuration** screen, provide the required license information and IP addresses and then click **Configure**.

Search panel

The **Search** panel displays the Search version, IP address for the Index Master node, and any alerts requiring user action. To load the Search console, click the **Search** link. Move the cursor to **Services** to view status information for Search services.

Figure 6 The **Search** panel on the ACM **Home** page

If Search was not configured during the initial configuration process, the panel displays a message indicating Search is not configured. To configure the Search node, click the message. The Search Configuration screen appears. On the **Search Configuration** screen, provide the required IP address and click **Configure**.

Configuring clients in Search

All the domains under Avamar get indexed automatically. Only those client domains that are added post deployment of DPSearch, will need to be added manually.

Cloud Disaster Recovery panel

The **Cloud Disaster Recovery** panel displays the CDRA version, and any alerts requiring user action. To load the Cloud Disaster Recovery console, click the **Cloud Disaster Recovery Web UI** link.

Figure 7 The **Cloud Disaster Recovery** panel on the ACM **Home** page

If CDRA was not configured during the initial configuration process, the panel displays **Click here to configure Cloud Disaster Recovery**, indicating that Cloud Disaster Recovery is not configured. To configure the Cloud Disaster Recovery node, click the message. The Cloud Disaster Recovery Configuration screen appears. On the **Cloud Disaster Recovery Configuration** screen, provide IP address and click **Configure**.

Note

- Do not change Avamar root user password before configuring CDRA from dashboard.
- Do not change DD boost user password before configuring CDRA from Dashboard.
- If cloud account and email address are not configured in CDRA configuration, the CDRA login page does not work. User has to configure cloud account and email address manually in CDRA.

Connect to the cloud account and add Cloud DR targets

Connect the CDRA to the Amazon Web Services account and add targets to the account.

Before you begin

- You have logged in to CDRA as administrator.
- You have an AWS account that is already configured before connecting to the cloud account.

Note

IDPA does the CDRA configuration automatically.

Procedure

1. Click **Cloud Account** on the menu bar.

   The **Connect to Cloud Account** page appears.
2. Click **Add Cloud Account**.
3. In the **Connecting to AWS Cloud account** dialog box, enter the access key and the secret key for the AWS account. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html provides information about obtaining the access and secret keys.
4. To copy the IAM policy, click **Copy IAM Policy**.

   This action copies to the buffer a JSON version of the minimum AWS user account permissions that are required for Cloud DR implementation, which can then be applied to AWS to set the permissions policy for the AWS user.
5. To view the Identity and Access Management (IAM) policy that represents the minimum AWS user account permissions that are required for Cloud DR implementation, click **Show IAM Policy**.
6. To save the AWS cloud account, click **Verify & Save**.

   The CDRA verifies that the account exists before saving the cloud account information and closing the **Connecting to AWS Cloud account** dialog box.

   Note

   When you have provided credentials to an AWS account, you cannot change to another AWS account.

Add cloud targets

You can add one or more cloud targets to the cloud account that includes selecting an Amazon S3 bucket and an encryption method.

Procedure

1. Click **Cloud Account** on the menu bar.

   The **Connect to Cloud Account** page appears.
2. Click **Add Cloud DR Target** to set up one or more Cloud DR targets on the cloud account.

   The Cloud DR target is the S3 bucket on AWS where data is written when VMs are backed up to the cloud. The Cloud DR Server is deployed on one of the targets.

The **Add Cloud DR Target** dialog box opens.

3. Enter a name for the Cloud DR target.

   The name entered here appears in the Avamar Administrator when creating a Cloud DR backup policy.

4. Select an Amazon S3 bucket for the Cloud DR target.
5. Click **Advance security option** and select an encryption method:

Option	Description
SSE-S3	Default encryption (no cost)
SSE-KMS	Key management service encryption (incurs a cost)

Note

If you select the SSE-KMS encryption method, only the default customer managed key is supported. Changing the encryption key might cause errors with the files in the Amazon S3 bucket.

For more information about these encryption methods, see:

- SSE-S3 - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html
- SSE-KMS - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

6. Click **Add**.

Deploy the Cloud DR Server

Deploy the CDRS on a on a specific Cloud DR target.

Before you begin

- Cloud DR targets are required in the AWS account before performing this task. Connect to the cloud account and add Cloud DR targets on page 21 contains information about adding Cloud DR targets to the AWS account.
- AWS Marketplace terms must be accepted before deploying the Cloud DR Server.

Procedure

1. Click Cloud DR Server on the menu bar.
   - If no CDRS has been deployed, the **Deploy Cloud DR Server** page appears.
   - If the CDRS has already been deployed, the **Cloud DR Server** page appears. You cannot deploy additional CDRS instances.
2. In the **Cloud DR Server Configuration** section, select the Cloud DR target on which to deploy the **Cloud DR Server**.
3. To allocate IP addresses for the Cloud DR solution, provide the **IPV4 CIDR Range**.
4. In the **User Configuration** section, enter and confirm passwords for the CDRS Admin and CDRS Monitor users.

   The passwords must:

- Be at least eight characters in length
- Contain characters of a minimum of three of the following types:
  - English uppercase: A-Z
  - English lowercase: a-z
  - Numeric character: 0–9
  - Special (non-alphanumeric) characters

a. Enter and confirm passwords for the CDRS Admin and CDRS Monitor users.

b. Enter an email address for DD Cloud DR password reset requests.

When the Cloud DR Server is successfully deployed, AWS sends an email to this address for verification. Follow the instructions in the email within 24 hours of deployment.

5. To confirm that you accept the marketplace terms, click the **I have accepted the AWS Marketplace terms** checkbox.

6. Click **Deploy** Cloud DR Server.

   The CDRA begins deployment of the CDRS to the Cloud DR target. If an error occurs during deployment, click **Cleanup** to delete the cloud resources that CDRS creates, and then retry deployment.

   Deploying the CDRS may take up to 30 minutes.

   If the deployment is successful, the Cloud DR Server page appears, listing the hostname of the CDRS host, and the region. Also deployed are:

   - A Virtual Private Cloud (VPC).
   - An Amazon Relational Database Services (RDS) catalog, to maintain persistent data.
   - A private subnet for communication between the RDS and CDRS.
   - A public subnet (Standard Mode) or private subnet (Professional Mode) with internet access to be used by CDRS.
   - The CDRS EC2 instance.

   The M4.Large instance type is used for the CDRS instance. To reduce deployment costs, you may want to purchase reserved instances from AWS; otherwise an on-demand instance is used. An elastic IP address is automatically assigned to the CDRS instance. You cannot change this IP address.

   Note

   Multiple Cloud DR Add-on appliances can connect to a single Cloud DR Server instance. However, one Cloud DR Add-on appliance cannot connect to multiple Cloud DR Server instances.

Results

When the CDRS is deployed, connect to the Cloud DR Server by clicking the CDRS hostname.

Create rapid recovery images for protected VMs

You can accelerate the recovery process ahead of time by creating rapid recovery images for protected VMs.

Creating a rapid recovery image starts the rehydration process and converts the VMDK files to an Amazon Machine Image (AMI). The recovery process then launches the recovered instance from the AMI.

Perform this procedure when a new backup copy is available in the Amazon S3 bucket.

Procedure

1. In the CDRS user interface, select **Protection > VM Protection** in the navigation pane.

   The existing protected VMs appear in the right pane. The **Rapid recovery image** column indicates whether the VM is enabled for rapid recovery.

2. Select one or more VMs and click **Create Rapid Recovery Image**.

Results

- The CDRS creates the AMI and removes any previous AMI for an earlier copy.
- You can verify the results by reviewing the **Rapid recovery image** column.
- You can disable rapid recovery for a VM by selecting it and clicking **Disable Rapid Recovery Image**.
- You can monitor the protection status and its progress by reviewing the **Protection status** column.

Perform a DR test or failover of a single VM

This procedure describes how to perform a DR test or failover on a single VM by using the Cloud DR Server interface.

Before you begin

To perform a DR test or failover of a VM by using the Cloud DR Server interface, you must have instances of virtual machines that are backed up by the on-premises backup software and copied to the cloud.

To ensure a successful failover, and better prepare for a disaster, best practices recommend testing various disaster recovery scenarios. After performing a DR test, you can promote the test to a failover.

When an operational error or disaster occurs on premises, you can fail over a VM to the public cloud. When the on-premise issue is resolved, you may fail the VM back to the on-premises environment.

Note

When performing failovers, you must fail over VMs in the correct order to ensure the continued operation of servers and applications.

Procedure

1. In the Cloud DR Server user interface, select **Recovery > VM Recovery**

   You can also open the **VM Recovery** page from the dashboard by clicking **See All** in the **Recovery** pane.

   The **VM Recovery** page appears.

2. Select the VM you want to recover and click **DR Test** or **Failover**.

   If you click **Failover** and the VM has never been tested, a message prompts you about this condition. Running a DR test is recommended before implementing a failover. The message also recommends that you shut down the production VM to avoid a possible data loss that is caused by accidental user access.

   Click **Select Copy** to continue.

3. On the **Copy and Network** window, select the VM copy and the network where you want to launch the EC2 instance.

   The **Advanced Options** section at the bottom of the window indicates the auto-selected EC2 instance type and security group to use for the recovery process.

4. If you do not want to use the auto-selected EC2 instance type or security group, expand **Advanced Options** and select an alternate EC2 instance type and one or more security groups.
5. Click **Start DR Test** or **Start Failover**.

Results

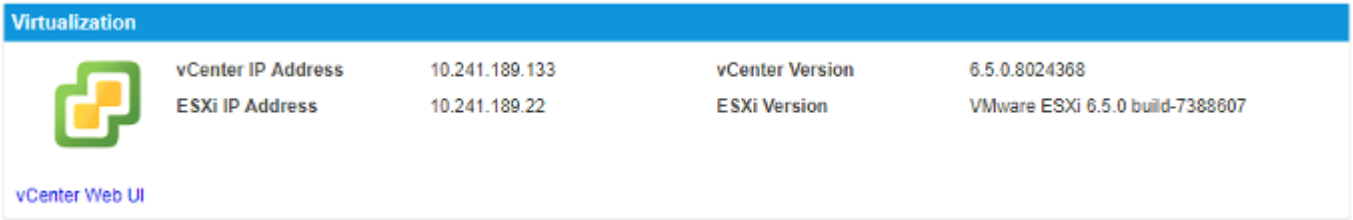
The recovery process begins and you can monitor progress on the **DR Activities** page. During the recovery process:

1. If the VM is not enabled for rapid recovery, a temporary Restore Service instance is launched in each region where recovery is needed. This instance performs hydration during recovery, and is automatically terminated after 10 minutes of idle time.
2. The Cloud DR Server then converts the VMDK to an AMI and launches an EC2 instance that is based on the AMI.
3. When the EC2 instance is running, the Cloud DR Server deletes the VMDK and AMI.

Virtualization panel

The **Virtualization** panel displays information about the internal virtual environment on the appliance, including the IP address and version of the vCenter server and ESXi host.

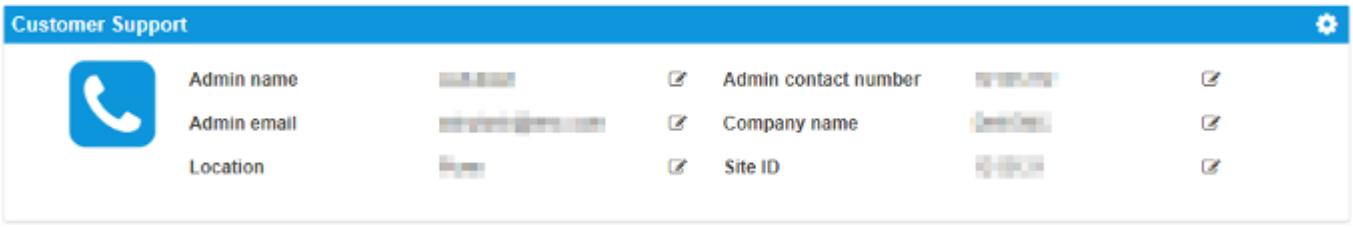
Figure 8 The **Virtualization** panel on the ACM **Home** page



Change customer contact information

The **Customer Support** panel displays the administrator contact and site information. To view the full value of an item, hover over the item.

Figure 9 The **Customer Support** panel on the ACM **Home** page



Procedure

1. In the **Customer Support** panel, click the **Edit** icon next to the value you want to change.
2. Type a new value:
   - **Admin Name**—Type the name of the administrator and click **Save**.
   - **Admin Number**—Type the phone number of the administrator and click **Save**.
   - **Admin Email**—Type the email address of the administrator and click **Save**.
   - **Company Name**—Type the name of the company and click **Save**.
   - **Location**—Type the location of the IDPA and click **Save**.
   - **Site ID**—Type the Site ID of the IDPA and click **Save**.

   You can verify your Site ID number on the Online Support website:

   a. Log in to the Online Support website with your credentials.

   b. Select **Service Center**.

   c. On the Service Center page, below the Sites and Contracts area, click **Administer a Site**.

   d. Ensure that the site where the storage system is installed is listed in the My Sites area.

Note

You can also search for a site and add it to the My Sites list. If a site ID is not available or the correct site ID is not listed, you must notify your local field representative to request one.

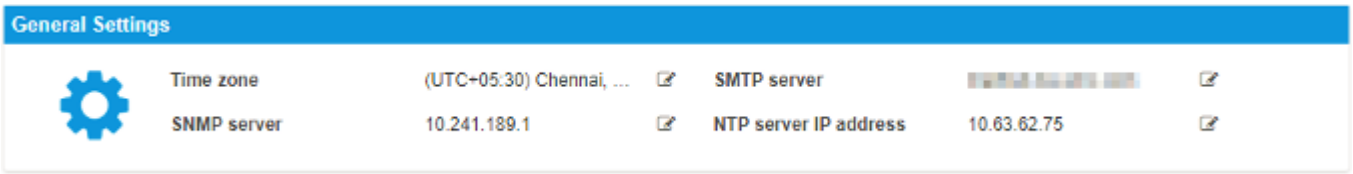
Results

Any new information that is provided is updated for the Backup Server node.

Change general system settings

The **General Settings** panel displays basic settings including time and network configuration. To view the full value of an item, hover over the item.

Figure 10 The **General Settings** panel on the ACM **Home** page



Procedure

1. In the **General Settings** panel, click the **Edit** icon next to the value you want to change.
2. Select or type a new value:
   - **Time Zone**—Select the time zone from the list and click **Save**. The time zone is updated for the Avamar, Data Domain, DP Advisor nodes, and Search nodes, the ACM, and the vCenter host server.

     NOTICE

     If this setting is changed, the Data Domain node restarts automatically.
   - **SMTP**—Type the SMTP server IP address and click **Save**. The SMTP server IP address is updated for the Avamar and Data Domain nodes and the vCenter host server.

     NOTICE

     If this setting is changed, the Avamar MCS and Backup Scheduler services restart automatically. Ensure that there is no backup running on the Avamar node before changing this setting.
   - **SNMP**—Type the SNMP server IP address and click **Save**. The SNMP server IP address is updated for the Avamar and Data Domain nodes and the vCenter host server.
   - **NTP**—Type the NTP server IP address and click **Save**. The NTP server IP address is updated for the Avamar, Data Domain, DP Advisor, and Search nodes, the ACM, and the vCenter host server.

     Note

     The NTP server must be specified by IP address. Do not use a server name in this field.
3. To change ACM DNS, perform the following step:
   a. Edit the `etc/resolv.conf` file, and then specify the IP address of the customer DNS server and the domain name.

      For example, when the customer environment has a public DNS server with an IP address of 10.254.66.23 and the domain name is mycompany.com, the `/etc/resolv.conf` file contains the following entries:

      Note

      The following output is an example, not the actual domain name and nameserver addresses. These values must be provided by the customer.

```
search mycompany.com
nameserver 10.254.66.23
nameserver 192.168.100.100
```

Note

Ensure that the entry for the public DNS server appears before the private DNS server. If the private DNS server appears first, the DPA integration with the Data Domain system will fail.

Configure external LDAP environment

By default, the application has the internal LDAP configuration. You can change the default configuration to an external LDAP environment.

Note

Ensure that you meet the following LDAP password requirements while configuring the external LDAP environment:

- Use only the following characters:
  - Letters (`A–Z`, `a–z`)
  - Numbers (`0–9`)
  - Period (`.`)
  - Hyphen (`-`)
  - Underscore (`_`)
- Contain at least one supported special character
- Be no longer than 20 characters

Procedure

1. Select **LDAP type**.
2. Check **Secure LDAP** to specify if the LDAP is secure.
3. Type **Server hostname**.
4. Type **Domain name**.

   Note

   The domain name can be alphanumeric characters and special characters (`-`, `_`, `.`, `=`, and `,`).

5. Type **Query username**.

   Note

   The query username can be alphanumeric characters and special characters (`-`, `_`, `.`, `=`, `,`, and `@`).

6. Type **Query password**.

Note

The query password should be minimum 9 to 20 characters, contains at least lower case alphabet, upper case alphabet, digit and any of these special characters—-, _, and ..

7. Type **Port number**.
8. Click **Validate** to check the validation of your LDAP details.
9. Click **Submit**., and then **Close**.

   The settings have been updated to external LDAP environment.

Note

After you configure LDAP to the external environment, you cannot revert to the default (internal) configuration.

10. Click **Close**.

Shut down the IDPA

Procedure

1. Use ssh to log in to AVE IP on the ACM dashboard. Use "admin" as user and the common password for the appliance.
2. From the root login, run the**/usr/local/avamar/bin/avinstaller.pl --checkPrcessingPackage** command to check if any package installation in progress on AVE or not. If it is, wait for package installation to complete.

```
root@xxxxxxx:/home/admin/#: /usr/local/avamar/bin/
avinstaller.pl --checkPrcessingPackage
roo@xxxxxxx:/home/admin
```

3. Run the **dpnctl status all** command. Examine the output and ensure that all important back up server services are up and running as shown in the following screen shot. If not, contact support.

```
admin@xxxxxxx~/>: dpcnt1 status all
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up
dpnctl: INFO: emt status: up
dpnctl: INFO: Backup scheduler status: up
dpnctl: INFO: Maintenance windows scheduler status: enabled
dpnctl: INFO: Unattended startup status: disabled
dpnctl: INFO: avinstaller status: up
dpnctl: INFO: ConnectEMC status: up
dpnctl: INFO: ddrmaint-service status: up
```

4. Run the **mccli checkpoint show** command to check all the checkpoints available on the Avamar system. Please take a screen shot of the output from running this command. The screen shot will be helpful in the later stages of the shutdown procedure.

```
admin@xxxxxxx:/home/admin/>:mccli checkpoint show
0,23000,CLI command completed successfully
Tag                    Time                Validated  Deletable
cp. 20180523033106 2018-05-23 09:01:06 IST Validated   No
cp. 20180523033444 2018-05-23 09:04:44 IST             No
cp. 20180523054859 2018-05-23 11:18:59 IST             No
```

5. Run the **mccli checkpoint create--override_maintenance_scheduler** command to create a checkpoint on AVE.

```
admin@xxxxxxx:/home/admin/>mccli checkpoint
create --override_maintenance_scheduler
0,22624, Starting to create a server checkpoint.
```

6. After the previous command executes, run the **mccli checkpoint show** on the AVE again to see the checkpoint tag which was newly created and assigned to the checkpoint you initiated in the previous step. the entry may take some time to get reflected in the output of this command (you may need to repeat this command 2-3 times). The newly created checkpoint entry can be validated from the timestamp associated with the entries. In the following screen shot, cp.20180523033444 is the tag of the newly created checkpoint.

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Tag                    Time                 Validated Deletable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST              Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

7. Run the following command **mccli checkpoint validate --cptag=<cp_tag_of_new_checkpoint> --override_maintenance_scheduler** to validate the checkpoint.

```
admin@xxxxxxx:/home/admin/>: mccli
checkpoint validate --cptag=cp.20180523033444 --
override_maintenance_scheduler
0,22612,Starting to validate a server checkpoijnt
Attribute    Value
tag         cp. 20180523033444
type        Full
```

8. Run the **mccli checkpoint show** command to check the status of the validation process of the checkpoint. The screen will display **In Progress** for an extended period of time. Wait until the screen displays a **Validated** status for the checkpoint tag.

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Tag                    Time                 Validated Deletable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST In Progress  Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Tag                    Time                 Validated Deletable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST Validated    Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

9. From the root login , run the **avmaint hfscheckstatus <checkpoint_tag> --ava**command to check the status of the job. If necessary, run the **avmaint hfscheck --checkpoint=<checkpoint tag> --ava** to perform an hfscheck on the checkpoint. Wait until above hfscheck job status command gives a completed status.

```
root@xxxxxxx:/home/admin/#:avmaint hfscheckstatus cp.
20180524033103 --ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheckstatus
nodes-queried="1"
nodes-replied="1"
nodes-total="1"
checkpoint="cp.20180524033103"
status="waitcomplete"
type="full"
checks="full"
elapsed-time="114"
start-time="1527154524"
end-time="0"
check-start-time="1527154524"
check-end-time="1527154562"
generation-time="1527154565"
stripes-checking="31"
stripes-completed="31"
offline-stripes="0"
minutes-to-completion="100.00">
<hfscheckerrors/>
</hfscheckstatus>
root@xxxxxxx:/home/admin/#:
```

```
root@xxxxxxx:/home/admin/#:avmaint hfscheck cp.20180524033103 --
ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheck
checkpoint="cp.20180524033103"
status="waitcgsan"
type="full"
checks="full"
elapsed-time="73"
start-time="1527154451"
end-time="0"
check-start-time="0"
check-end-time="0"
generation-time="1527154524"
percent-complete="0.00">
<hfscheckerrors/>
</hfscheck>
```

```
root@xxxxxxx:/home/admin/#:avmaint hfscheckstatus cp.
20180524033103 --ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheckstatus
nodes-queried="1"
nodes-replied="1"
nodes-total="1"
checkpoint="cp.20180524033103"
status="completed"
result="OK"
type="full"
checks="full"
elapsed-time="103"
start-time="1527154451"
end-time="1527154554"
check-start-time="1527154524"
check-end-time="1527154554"
generation-time="1527154651"
stripes-checking="31"
stripes-completed="31"
offline-stripes="0"
percent completion="100.00">
<hfscheckerrors/>
</hfscheckstatus>
```

10. Run the **dpcntl stop sched** command to stop all the backup job that will be scheduled by AVE(current jobs will still continue to run).

```
admin@xxxxxxx:~/>: dpnctl stop sched
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: Suspending backup scheduler...
dpnctl: INFO: Backup scheduler suspended.
```

11. Run the **dpnctl stop maint**command to stop maintenance services running on Avamar.

```
admin@xxxxxxx:~/>: dpnctl stop maint
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: Suspending maintenance windows scheduler...
dpnctl: INFO: Maintenance windows scheduler suspended.
```

12. From the root login, run the **cplist** command and verify the following:

    a. Check if hfschecked checkpoint is present within 36hrs of time.

    b. Check whether there is a hfs entry for at least one checkpoint which was created within last 36hrs of time.

```
root@xxxxxxx://ust/local/avamar/bin/#: cplist
cp. 20180524033103 Thu May 24 09:01:03 2018 valid hfs --- nodes
1/1 stripes  32
cp. 20180524033441 Thu May 24 09:04:03 2018 valid hfs --- nodes
1/1 stripes  32
```

13. Run the **avmaint sessions** on AVE. This stops all active sessions on Avamar. It will list all the sessions currently running on AVE. To kill each session, select the **sessionid** and run the **avmaint kill <sessionid>' command**. Do this for every session until no session entries are found on AVE.

```
admin@xxxxxxx://>: avmaint sessions
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<nodesessionlist count="1">
<sessionlist
id="0.0"
count="1"
<session
numthreads="1"
type="avtarbackup"
ndispatchers="1"
expires="1532240626"
domain=""
workorderid="MOD-1527056601340"
pidnum="1001"
numconns="1"
path="/clients/acmpun059.lss.emc.com"
starttime="1527056651"
encrypt=="tls-sa"
dispatcher0="xxxxxxxxxxxxxx"
sessionid="9152705660134709"
root="/"
pluginid="Unix"
encrypt-strength="high"
clientid="86752318de80049804395b0756fde3fa034a9846"
user=""
clientip=xxxxxxxxxxxxx>
<host
numprocs="4"
speed="16777200"
osuser="root"
name="xxxxxxx"
memory="32175">
<build
```

```
msgversion="13-10"
time="06:46:59"
appname="avtar"
zlibversion="1.2.8"
lzoversion=1.08 Jul 12 2002"
date "Mar 22 2018"
appversion="7.5.101-101_HF294929"
processortype="x86_64"
osversion="SLES-64"
sslversion="TLSv1 OpenSSL 1.0.2a-fips 19 Mar 2015
osname="Linux"/>
```

```
admin@xxxxxxx://>: avmaint kill 9152705692533109
kill: killed 9152705692533109
```

```
admin@xxxxxxx:/home/admin/>: avmaint sessions
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<nodesessionlist count="1">
<sessionlist
id="0.0"
count="0"/>
</nodesessionlist>
```

14. From the Avamar root login, run the **avmaint cpstatus**to verify that no checkpoint is in progress. Verify that all the checkpoints listed are in a completed state. Wait for checkpoints to complete if they are running.

```
roor@xxxxxxx://#: avmaint cpstatus
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cpstatus
generation-time="1527099528"
tag="cp.20180523055705"
status="completed"
stripes-completed="32"
stripes-total="32"
start-time="1527055025"
end-time="1527055044"
result="OK"
refcount="1"/>
```

15. Run the **avmgr getb --path=/MC_BACKUPS --mr=1 --format=xml**to verify that the MCS has been flushed within the last 12 hours. You can check the actual time of the MCS flush by running the **t.pl <time_tag>** entry (execute in /usr/local/avamar/bin directory). If the MCS has not been flushed in the last 12 hours, run the **mcserver.sh- -flush**' to flush the MCS on AVE.

```
admin@xxxxxxx:~/>: avmgr getb  --path=/MC_BACKUPS --mr=1 --
format=xml
1 Request succeeded
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<backuplist version="3.0">
<backuplistrec flags="32768001" labelnum="418" label=""
created="157174902"
roothash="587c90ceea90e7523366025b3955a8ed142170f"
totalbytes="48514156.00"
ispresentbytes="0.00" pidnum="1001" percentnew"0" expires="0"
created_prectime="0x1d3f371fd3ffb5a" partial="0"
retentiontype="daily,weekly,monthly,yearly
backuptype="full" ddrindex="0" locked="1" direct_restore="1"
tier="0"
appconsistent="not_available"/>
</backuplist>
```

```
admin@xxxxxxx:~/>: mcserver.sh--flush
=== BEGIN === check.mcs (preflush)
check.mcs     passed
=== PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Adminstrator Server Flushed.
```

```
admin@xxxxxxx:~/>: avmgr getb  --path=/MC_BACKUPS --mr=1 --
format=xml
1 Request succeeded
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<backuplist version="3.0">
<backuplistrec flags="32768001" labelnum="419" label=""
created="157178362"
roothash="5876c90ceea90e7523366025b3955a8ed1422170f"
totalbytes="48514156.00"
ispresentbytes="0.00" pidnum="100" percentnew"0" expires="0"
created_prectime="0x1d3f371fd3ffb5a" partial="0"
retentiontype="daily,weekly,monthly,yearly
backuptype="full" ddrindex="0" locked="1" direct_restore="1"
tier="0"
appconsistent="not_available"/>
</backuplist>
```

```
admin@xxxxxxx:~/>:/usr/local/avamar/bin/>: t.pl 1527178362
local: Thu May 24 21:42:42 2018   gmt: Thu May 24 16:12:42 2018
```

```
admin@xxxxxxx:~/>: mcserver.sh--flush
=== BEGIN === check.ms (preflush)
check.mcs
===PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Administrator Server Flushed
```

16. In the /usr/local/avamar/bin directory, run the **hfscheck_kill** to kill the hfscheck jobs (if there are still any running).

```
admin@xxxxxxx:/usr/local/avamar/bin/#: hfscheck_kill
Using /usr/local/avamar/ver/probe.xml
```

17. Run the **avmaint gckill --ava** command to kill all garbage collector jobs.

```
admin@xxxxxxx:/usr/local/avamar/bin/#: avmaint gckill --ava
```

18. Run the **dpnctl shutdown --precheck** command to check whether all the shutdown requirements are satisfied.

```
admin@xxxxxxx:~/>: dpnctl shutdown --precheck
Identity added /home/admin/.ssh/admin_key)
dpnctl: INFO: Checking for validated checkpoint
dpnctl: INFO: found the most recently validated checkpoint: cp.
20180523033444 at
'Wed May 23 03:34:44 2018 UTC'
dpnctl: INFO: VALIDATED CHECKPOINT PASSED
dpnctl: INFO:
[###############-----------------------------------20%]
dpnctl: INFO: Starting MCS flush check
dpnctl: INFO: Last MCS flush at 'Wed May 23 15:45:02 2018'
dpnctl: INFO: LAST MCS PASSED
dpnctl: INFO:
[###############-----------------------------------30%]
dpnctl: INFO: Checking for file system and gsan percentage
dpnctl: INFO: FS/GSAN PERCENTAGE PASSED
dpnctl: INFO:
[###############-----------------------------------50%]
dpnctl: INFO: GSAN tasks: idle
dpnctl: INFO: Checking for hfscheck.
dpnctl: INFO: No hfsceck maintenance task is running.
dpnctl: INFO:
[###############-----------------------------------70%]
dpnctl: INFO: Checking for GC.
dpnctl: INFO: No GC task is running.
dpnctl: INFO:
[###############-----------------------------------80%]
dpnctl: INFO: Checking for active sessions (backup/restore).
dpnctl: INFO: No backup/restore is running.
dpnctl: INFO:
[###############-----------------------------------90%]
```

```
dpnctl: INFO: Checking for active checkpoint.
dpnctl: INFO: No checkpoint task is running.
dpnctl: INFO:
[###############-----------------------------------100%]
```

19. Perform file system cleaning by running the following CLI command on the Data Domain manager:

```
filesys clean status
```

20. Verify passwords are synchronized. Changing a password for a component causes the ACM UI to display the password out of sync error message. Ensure that all passwords are synchronized by checking each panel in the dashboard. If any password is not synchronized, the shutdown process cannot start. To allow the ACM to gather health information for the component, you must update the stored password in the ACM UI to match. To update an unsynchronized password, click the error text.
21. On the dashboard **Home** tab, click the **Shutdown Appliance** icon.
22. Type the administrator password, click **Authenticate**, and then click **Yes**.
23. Click **Logout**.

    ⚠ CAUTION

    It will a long time (estimated 45 minutes) between the ACM going down and the system physically powering off.

    While the appliance is shutting down, the **Login** screen displays a message indicating shutdown is in progress. To view the status, Log into ESX to monitor the shutdown.

Health

The **Health** tab displays status information and alerts for the following hardware components of the IDPA:

- DP4400 servers
- vCenter

The IDPA uses Secure Remote Services to automatically send critical and fatal events to Customer Support for troubleshooting. A support ticket is opened based on the events that are received. Critical and fatal events are sent to Customer Support either after 30 min have elapsed, or when 30 events have accumulated, whichever occurs first.

By default, all events are deleted after 30 days. If no events have occurred in the selected time period, the **Event Summary** and **Event Details** panel indicate that there is no data available.

Event Summary

The **Event Summary** panel displays a summary of the status events on the appliance, grouped by **Device** and **Severity**.

To change the time period for which events are displayed, select an option from the **Event summary for** box. Selecting **Today** lists events that have occurred from midnight to the present.

To show only events for a specific device or of a specific severity in the **Event Details** panel, click the corresponding wedge in the chart.

Event Details
The **Event Details** panel displays a paginated list of the status events on the appliance. Use the **Device** and **Severity** boxes to filter the list by Device, Severity, or both. To read more detailed information about an event, click its table entry. To export the list as a CSV file, click the CSV icon.

Troubleshooting
If a critical component of the health monitoring function is not working, the panels indicate that the service is down and an error message is displayed at the top of the page. For more information about how to resolve issues with the **Health** tab, see Troubleshooting health monitoring on page 50.

Upgrade

The **Upgrade** tab allows an administrator to update the IDPA software. Refer to Update the IDPA software on page 43 for more information.

Start up the IDPA

You can start the IDPA from Dell server or through iDRAC.

Start up the IDPA from Dell server

Switch on the power button present on the Dell server.

Note

No other action is required to start the IDPA model DP4400.

Start up the IDPA from iDRAC

Procedure

1. Turn on the iDRAC and log in to iDRAC from its UI using `root` user and iDRAC password.
2. Click the **Power On System** button.

   Note

   The ESX UI will be accessible within a maximum time of 15 minutes.

3. Login to ESXi UI.

   The ESX exits from maintenance mode and the DataProtection-ACM VM starts all the VMs present in IDPA in the following order, by default:

   a. DataProtection-VSCA
   b. DataProtection-ACM
   c. DDVE
   d. AVE
   e. DPC
   f. DPADatastoreServer

g. DPAApplicationServer

h. DPSIndexMaster

i. CDRA

j. AVProxy

Note

You can also observe the activity from the **Recent tasks** section at the bottom of ESX UI page.

4. Connect to the ACM by accessing the *https://<ACM_IP>:8543* URL from the browser.

Access components with a browser

In addition to clicking the links in the ACM panels, you can access the user interface for individual components by browsing to the corresponding network location and typing the username and password.

In each of the following sections, *<component_ip>* refers to the IP address of the component. The credentials for Search and IDPA System Manager are determined by your LDAP setup.

Note

Ensure you are using Flash version 27.0.0.183 or later to access the vCenter web client.

Component	Location	Username
Avamar client manager	`https://<component_ip>/aam`	`MCUser`
Avamar user interface	`https://<component_ip>/mcui`	`MCUser`
Avamar SSH login		`admin`
Data Domain user interface	`https://<component_ip>`	`sysadmin`
IDPA System Manager user interface	`https://<component_ip>`	`<username>@<domain>` **Note** If external LDAP has not been configured, then the username is `idpauser`, by default.
DP Advisor user interface	`https://<component_ip>:90502/dpaui/jsp`	`administrator`
Search user interface	`https://<component_ip>/admin/#/login`	`<username>@<domain>`

Component	Location	Username
		Note If external LDAP has not been configured, then the username is `idpauser`, by default.
vCenter web client	`https://<component_ip>`	`idpauser`

User accounts for components

The IDPA configuration uses the user accounts in Table 4 on page 38. By default, these accounts use the common IDPA password . For information on how to change component passwords, refer to Change passwords and synchronize components on page 39.

Table 4 Component and user account mapping

Component	Using SSO	Username	Password
ACM	No	root	Common password provided during DP4400 configuration.
IDPA System Manager (If external LDAP is not configured)	No	idpauser	Common password provided during DP4400 configuration.
IDPA System Manager (If external LDAP is configured)	No	Respective LDAP credentials	External LDAP password as applicable.
Avamar	Yes	NA	SSO will take care of this logging in automatically.
Data Domain	No	sysadmin	Common password provided during DP4400 configuration.
Data Protection Advisor	No	administrator	Common password provided during DP4400 configuration.
Search	Yes	NA	SSO will take care of this logging in automatically.
CDRA	No	admin	Common password provided during DP4400 configuration.
CDRS	No	admin or monitor	Password set during CDRS deployment.
vCenter	No	idpauser	Common password provided during DP4400 configuration.
ESXi	No	idpauser	Common password provided during DP4400 configuration.

Change passwords and synchronize components

Single click user password change is one of the new features introduced in DP4400. It is recommended that you use the feature for changing the password as it changes passwords for all the components in the IDPA.

Note

Changing passwords of individual components is not recommended. Due to any unforeseen circumstances, if you have to change passwords of individual components, refer the following section.

Changing passwords for individual components
Some changes to component passwords and settings require updating the settings of other components.

Changing a password for a component causes the ACM UI to display the `password out of sync` error message. To allow the ACM to gather health information for the component, you must update the stored password in the ACM UI to match. To update an unsynchronized password, click the error text.

Data Domain settings

Updating the Data Domain password
For information about how to change the Data Domain `sysadmin` account password, refer to the *Data Domain Operating System Administration Guide*. After changing the password for the `sysadmin` account, log in to DP Advisor and update the Data Domain SSH credentials to match.

NOTICE

Update the Data Domain SSH credentials in DP Advisor immediately. Failure to do so can cause account lockout as DP Advisor repeatedly tries to connect with the old password.

After updating the password in DP Advisor, log in to the ACM and update the **Protection Storage** password to match.

Note

Do not change DD boost user password before configuring CDRA from Dashboard.

Avamar settings

Updating Avamar passwords
Avamar uses multiple user accounts, including `MCUser`, `viewuser`, server `root`, OS `admin`, and OS `root`. The IDPA requires that the OS `admin` and OS `root` accounts use the same password. The `MCUser`, `viewuser`, and server `root` accounts must also share a password, which can be different than the OS `admin` and OS `root` password. For more information about how to change an Avamar password, refer to the *Avamar Administration Guide*.

After changing the password for any Avamar account, log in to the ACM and update the **Backup Server** password to match.

If you change the `MCUser` account password, update it in the Search Admin UI. For more information about how to change the Avamar password for Search, refer to the *Data Protection Search Installation and Administration Guide*.

If you change the `viewuser` account password, update it in the DP Advisor UI. For more information about how to change the Avamar password in DP Advisor, refer to the *Data Protection Advisor Installation and Administration Guide*.

Updating the DD Boost user password

After changing the password for the Data Domain `DDBoostUser` account, log in to the **Avamar Administrator** GUI. Edit the Data Domain system settings and update the DD Boost user password to match. For more information, refer to the "Editing a Data Domain system" procedure in the *Avamar Administration Guide*.

Note

Do not change DD boost user password before configuring CDRA from Dashboard.

DP Advisor settings

Updating DP Advisor passwords

To change the DP Advisor `administrator` account password or `root` password, you must log in and change that password for each DP Advisor node. For more information about how to change a password in DP Advisor, refer to the *Data Protection Advisor Installation and Administration Guide*.

After changing the password on all nodes, log in to the ACM and update the **Reporting and Analytics** password to match.

Updating the Data Domain SNMP community string

If the community string is changed from its default value of *public*, DP Advisor must be updated to reflect the change.

1. Log in to Data Domain and change the community string with the following command, where *<community_string>* is the new string and *<Dpa_DC_Agent_IP>* is the IP address of the Data Collection Agent VM.

   ```
   snmp add rw-community
   <community_string> hosts
   <Dpa_DC_Agent_IP>
   ```

2. In the **Reporting and Analytics** panel of the ACM, click the **Reporting and Analytics Web UI** link.
3. Click **Manage Credentials** on the **Admin** > **System** page.
4. Select the **EMC Data Domain Credential** and update the community string to match.

DPSearch settings

Updating the DPSearch password

To change the Search OS `root` password, you must log in and change the OS `root` password for each Search node. For more information about how to change the OS `root` password, refer to the *Data Protection Search Installation and Administration Guide*.

After changing the password for the Search OS `root` account, log in to the ACM and update the **Search** password to match.

Note

#, **?**, **/**, and **** are illegal characters for new passwords.

Updating the LDAP configuration for DPSearch

If the LDAP query user password is changed, it may not be possible to log in to the DPSearch Admin UI. To update this password, refer to the referenced procedures in the *Data Protection Search Installation and Administration Guide*.

1. The first time you log in to a Search node with SSH, you must accept the EULA. For more information, refer to the "Initializing the Data Protection Search environment" procedure in the *Data Protection Search Installation and Administration Guide*.
2. After accepting the EULA, select the option `[2] Configure Network Settings` and then press **F9** to quit.
3. When the system displays `Do you want to reboot now? y(es) or n(o):`, type **no**.
4. To update the LDAP configuration, complete the "Updating LDAP configuration in the Data Protection Search Admin installation script" procedure in the *Data Protection Search Installation and Administration Guide*.
5. Repeat steps 1–4 for each Search node.
6. Log in to each Search Index Data Node with SSH and run the command **service unicorn restart**.
7. Log in to the Search Index Master Node with SSH and run the command **service unicorn restart**.

CHAPTER 3

Update the IDPA software

This chapter describes how to update the software of the IDPA.

Topics include:

Update the appliance software

Update the software for the IDPA from the **Upgrade** tab of the ACM.

Once the software update file is downloaded and copied to the `/data01/upgrade` directory, the package file is automatically detected and appears in **Upgrade Binary Location**.

CHAPTER 4

Troubleshooting

This chapter contains basic troubleshooting information to help resolve possible issues.

Topics include:

System log files

To help troubleshoot issues, download bundled log files for the IDPA from the **Home** tab page directly. Select the **Download log bundle** option from the log bundle icon available on the **Home** tab page to download the log files. The log files for the specified components are saved in the folder `/Downloads/` on the system in a compressed format.

Note

The user should not create or copy their logs in `/data01/log_bundle` folder as this functionality deletes all existing log while creating log bundle.

Troubleshooting startup

If one part of the startup process fails to complete automatically, the problem can be resolved manually to allow startup to continue.

Avamar does not start

If Avamar does not complete startup, connect to the Avamar server. If Avamar reports that GSAN did not shut down cleanly, select the option to roll back to the last checkpoint.

The ACM does not start

If the ACM service does not start within 2 hours and 15 minutes of powering on the appliance, one or more of the following components are not powered on or are not accessible on the network:

- Data Domain
- AVE

The Data Domain component must be powered on and accessible before the ESXi host is powered on.

1. Verify that the components that are required for the configuration are powered on.
2. Verify that the required components are accessible on the network. Resolve any connectivity issues that are encountered.
   - If the ACM loads successfully, skip the rest of this procedure. The Search nodes, DP Advisor nodes, IDPA System Manager, AVE, and Avamar Proxy start automatically.
   - If all required components are powered on and accessible, but the ACM does not load, restart the ACM service:
3. Stop the `dataprotection_webapp` service:
   `service dataprotection_webapp stop`
4. Start the `dataprotection_webapp` service:
   `service dataprotection_webapp start`

The Search nodes, DP Advisor nodes, IDPA System Manager, AVE, and Avamar Proxy start automatically.

The VMs do not start

When switch the power button on present on the Dell Server, the ACM internally executes `local.sh (/etc/init.d/local.sh)` and the VMs start automatically. To start the VMs manually:

1. Move ESXi out of maintenance mode manually.

   Note

   To do this, log in to ESX using `idpauser` and select **Exit maintenance mode**.

2. Start the DataProtection-VCSA by running the `/etc/init.d/local.sh` script on ESXi or power on the VM from the ESXi.
   DataProtection-ACM VM starts five minutes after the VCSA VM starts.
3. If DDVE VM is not up, click the **Power on** button to start the DDVE VM.
   Code waits filesystem status to show up and running.
4. If AVE is not started, start AVE VM from ESX UI.
5. login to AVE using admin credentials.
   ACM executes `dpnctl status all`, `dpnctl start all`, and `dpnctl start maint` commands.
6. If something goes wrong, execute the following in sequence and click the **Power on** button:
   - DataProtectionSearch Vapp
   - DPADatastoreServer VM
   - DPAApplicationServer VM
   - DataDomainCloudDR VApp
   - DataProtectionCentral VApp
   - AVProxy VM

   Note

   Check the status of DPA services by running `/opt/emc/dpa/services/bin/dpa.sh service status` command after logging in to Datastore server using its IP, OS user `root` and its password.

7. If DPS vApp does not started, start vApp.
8. Start the services of search by logging in to index master IP using OS root credentials and executing following commands:
   a. `service elasticsearch start`
   b. `service search-cis-core start`
   c. `service search-cis-schedule start`
   d. `service search-networker-worker start`
   e. `service search-networker-action start`
   f. `service search-avamar-worker start`
   g. `service search-avamar-action start`
   h. `service search-worker start`
   i. `service search-adminapi start`
   j. `service search-api start`
9. Login to VCSA using `idpauser`credentials, select **AVProxy** VM and click the **Power on** button.
10. After IDPA starts, start two services of Avamar using `dpnctl start emt`.

Adding a CA-signed certificate

The ACM includes a self-signed certificate, which may cause the browser to report an unsecured connection. To resolve this issue, replace the default certificate with a CA-signed certificate.

Before you begin

- Access the IDPA command line using one of the following procedures:
  - Log in to vCenter, right-click the DataProtection-ACM VM, and select **Open Console**. Type the ACM credentials.
  - Connect to the ACM by using an SSH client to access its IP address. Type the ACM credentials.
- Change the directory to `/root`

Procedure

1. Stop the Tomcat server.

   ```
   service dataprotection_webapp stop
   ```

2. Back up the existing keystore file.

   ```
   cp /root/.keystore /root/.keystore.bkp
   ```
   Use the backup if you encounter any errors in this process.

3. Delete the existing self-signed certificate from the keystore.

   ```
   /usr/java/latest/bin/keytool -delete -alias tomcat -storepass
   changeit
   ```

4. Create a new certificate.

   ```
   /usr/java/latest/bin/keytool -genkeypair -v -alias tomcat -
   keyalg RSA -sigalg SHA256withRSA -keystore /root/.keystore -
   storepass changeit -keypass changeit -validity 3650 -dname
   "CN=idpa.companyname, OU=Idpa, O=CompanyName, L=Hopkinton,
   S=Massachusetts , C=US"
   ```

5. Generate a CSR file for the keystore.

   ```
   /usr/java/latest/bin/keytool -certreq -alias tomcat -keyalg RSA
   -file /root/ACM_Host.csr -keystore /root/.keystore
   ```

6. Get the CA-signed certificate in the .p7b format by using the CSR content and save the certificate.
7. Import the new certificate into the keystore.

   ```
   /usr/java/latest/bin/keytool -import -alias tomcat -file /root/
   certnew.p7b -keystore /root/.keystore
   ```

8. To ensure `/usr/local/dataprotection/tomcat/conf/server.xml` is using the `/root/.keystore` file, check the value of the `keystoreFile` attribute for the HTTP Connector.
9. Verify the certificates in the keystore.

   ```
   /usr/java/latest/bin/keytool -list -keystore /root/.keystore -
   alias tomcat
   ```

10. Start the Tomcat server.

    ```
    service dataprotection_webapp start
    ```

Configure secure AD having self-signed Certificates on IDPA

If you are using secure AD with self-signed Certificates, search fails to configure if the self-signed certificate is not present on search VM.

Procedure

1. Export root CA certificate.

   Refer https://support.microsoft.com/en-us/help/555252 to know how to export the root CA certificate.
2. Log into the Root Certification Authority server or Active Directory Server with administrator account.
3. Go to**Start** > **Run**, type `cmd`, and press **Enter**.
4. To export the Root Certification Authority server into a new file name `ca_name.cer`, run `certutil -ca.cert ca_name.cer`.
5. Convert certificate as PEM format as follows:
   a. Cy `ca_name.cer` to Search Master.
   b. Run `openssl x509 -in ca_ name.cer -inform der -out ca_name.pem -outform pem`.
   c. Copy this `ca_name.pem` to `/etc/pki/trust/anchors/` on Search Node.
6. Do LDAP Configuration from Dashboard.

Troubleshooting Avamar

If there is a problem with Avamar, the **Backup server** panel in the ACM dashboard displays the following status:

```
Backup Agents Installation in progress...
```

Possible causes for this issue include:

- The Avamar service, Avamar, or AVE is down.
- Avamar cannot be pinged.
- There is a mismatch between the Avamar administrator password and the password stored in the ACM.

The Avamar service is down

To start the Avamar service:

1. Using an SSH client, connect to the Avamar Utility node as the admin user.
2. Type the command `dpnctl start all`

Avamar or AVE is down

Power on the Avamar or AVE server.

Avamar cannot be pinged
If Avamar cannot be pinged, find and resolve the source of the issue. Possible causes include:

- The Avamar server is down.
- There is a network connectivity issue.
- The Avamar server has a hardware issue.

Credential mismatch
To resolve a password mismatch, click the warning message in the **Backup server** panel and provide the correct password.

Troubleshooting health monitoring

If there is an issue with SNMP or one of the health monitor processes, the **Health** tab cannot display data.

SNMP validation errors
By default, the ACM validates the SNMP configuration of the switch and Dell servers every 4 hours. If the ACM detects that the SNMP configuration for a component is disabled or missing, it automatically corrects the configuration.

If the ACM cannot reach one of the components on its internal IP, the following message is displayed on the **Health** tab: `Failed to validate SNMP configuration on component(s) <unreachable-component>`

To resolve this issue:

1. Verify that the internal IP addresses of DP4400 server is reachable on the network.
2. If the component is reachable on the network, verify SSH connectivity by attempting to connect with the default SSH password. If an SSH connection cannot be established, revert the SSH password on the component to the default password.

Note

Refer Changing passwords and synchronizing components to know how to change passwords and synchronize components.

Health monitor processes errors
If the SNMP Receiver port, Message Broker service, or Database service is down, the following message is displayed on the **Health** tab: `Health monitor processes are down : <process>`

To resolve this issue, connect to the ACM using SSH and follow the procedure that corresponds to the error message:

- If the SNMP Receiver port is down, verify that port 161 is enabled. If the port is enabled and the problem persists, restart the Tomcat service with the following command:

```
service dataprotection_webapp restart
```

- If the Message Broker service is down, verify that the RabbitMQ service is running with the following command:

  ```
  service rabbitmq-server status
  ```

  If the service is not running, start it with the following command:

  ```
  service rabbitmq-server start
  ```

- If the Database service is down, verify that the PostgreSQL service is running with the following command:

  ```
  service dataprotection_database status
  ```

  If the service is not running, start it with the following command:

  ```
  service dataprotection_database start
  ```

CHAPTER 5

Additional resources

This chapter provides references to other materials related to the IDPA and individual components.

Topics include:

Document references for the IDPA

The IDPA documentation set includes the following publications:

- *Integrated Data Protection Appliance DP4400 Installation Guide*
  Instruction for installing the IDPA DP4400 hardware.
- *Integrated Data Protection Appliance DP4400 Getting Started Guide*
  Explains how to perform initial IDPA configuration tasks and how to get started with basic functionality like backup and restore.
- *Integrated Data Protection Appliance Product Guide*
  Provides the overview and administration information about the IDPA system.
- *Integrated Data Protection Appliance Release Notes*
  Product information about the current IDPA release.
- *Integrated Data Protection Appliance DP4400 Service Procedure Guide*
  Procedures for replacing or upgrading hardware components of the IDPA.
- *Integrated Data Protection Appliance Security Configuration Guide*
  Information about the security features that are used to control user and network access, monitor system access and use, and support the transmission of storage data.
- *Integrated Data Protection Appliance Software Compatibility Guide*
  Information about software components and versions used in the IDPA product.

Document references for individual components

The documentation for these components can be obtained from Online Support at https://support.emc.com.

Protection Storage node
The following document contains information that is related to Data Domain:

- *Data Domain Operating System Administration Guide*
  This publication explains how to manage Data Domain systems with an emphasis on procedures using the Data Domain System Manager.

Backup Server node
The following documents contain information that is related to Avamar:

- *Avamar Administration Guide*
  This publication describes how to configure, administer, monitor, and maintain an Avamar server.
- *Avamar and Data Domain System Integration Guide*
  This guide includes procedures for configuring the Avamar server to perform cloud tier operations on the Data Domain system.
- *Avamar for VMware User Guide*
  This publication describes various methods and strategies for protecting VMware virtual machines.
- *Avamar NDMP Accelerator for Oracle ZFS User Guide*
  This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported Oracle ZFS storage appliances.
- *Avamar NDMP Accelerator for NetApp Filers User Guide*

This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported NetApp filers.

- *Avamar NDMP Accelerator for EMC NAS Systems User Guide*
  This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported EMC Isilon, Unity, VNX, VNXe, and Celerra systems.
- *Avamar for VMware User Guide*
  This publication describes various methods and strategies for protecting VMware virtual machines.

IDPA System Manager node

The following documents contain information that is related to Integrated Data Protection Appliance System Manager:

- *IDPA System Manager Release Notes*
  Contains the most up-to-date information about the current release.
- *IDPA System Manager Getting Started Guide*
  This document includes information about how to deploy Integrated Data Protection Appliance System Manager, and then get started with Integrated Data Protection Appliance System Manager administration.
- *IDPA System Manager Administration Guide*
  This document includes information about how to administer Integrated Data Protection Appliance System Manager.
- *IDPA System Manager Security Configuration Guide*
  This document includes information about security features and capabilities of Integrated Data Protection Appliance System Manager.

Reporting and Analytics node

The following documents contain information that is related to Data Protection Advisor:

- *Data Protection Advisor Installation and Administration Guide*
  This publication describes how to install, maintain and configure DP Advisor.
- *Data Protection Advisor Product Guide*
  This document provides information on how to use the DP Advisor web console to run and create reports, view alerts, and view the status of replication operations.

Search Storage

The following document contains information that is related to Data Protection Search:

- *Data Protection Search Installation and Administration Guide*
  This publication describes how to install, maintain and configure Search.

Cloud Disaster Recovery

The following documents contain information that is related to DD Cloud DR and CDRA.

- *Data Domain Cloud Disaster Recovery Release Notes*
  Contains supplemental information about DD Cloud DR and the most up-to-date information about the current release.
- *Data Domain Cloud Disaster Recovery Installation and Administration Guide*
  This document describes how to install, deploy, and use the DD Cloud DR product.

IDPA training resources

Video walkthroughs, demonstrations, and explanations of product features are available online.

You can obtain additional IDPA training and information at https://education.emc.com, such as:

- Integrated Data Protection Appliance 2.2 DP4400 Overview
- Integrated Data Protection Appliance 2.2 DP4400 Getting Started
- Integrated Data Protection Appliance 2.2 DP4400 CRU Maintenance
- Integrated Data Protection Appliance 2.2 System Manager Overview
- Integrated Data Protection Appliance 2.2 Alert Monitoring